IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Bruce Wallace, et al.	Examiner:	N. Patel
Serial No.:	10/615,513	Art Unit:	2435
Conf. No.:	9214		
Filed:	July 8, 2003	Attorney Docket No.:	15929ROUS02U
Title:	DISTRIBUTED SECURITY FOR INDUSTRIAL NETWORKS		

CERTIFICATE OF ELECTRONIC TRANSMISSION

I hereby certify that this document, along with any other papers referred to as being attached or enclosed, is being filed electronically on June 8, 2009.

/John C. Gorecki/

John C. Gorecki, Reg. No. 38,471

M.S. Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF

(i) Real Party In Interest

This application is owned by Nortel Networks, Limited, of St. Laurent, Quebec, CANADA.

(ii) Related Appeals and Interferences

None

(iii) Status of Claims

Claims 1-7, 9-11, and 13-25 are pending in this application and stand rejected. Claims 8 and 12 have been cancelled. The rejection of all pending claims under 35 USC 103 is appealed.

(iv) Status of Amendments

The amendments submitted by applicant on July 9, 2008 have been entered (See Final Office Action dated October 23, 2008, page 2). Applicants filed a notice of appeal in response to receipt of the final office action and have not filed another paper in response to the Final Office Action dated October 23, 2008. Accordingly, there are no un-entered amendments.

(v) Summary of Claimed Subject Matter

Programmable Logic Controllers (PLCs) are programmable devices that allow the operation of factory machines to be altered by adjusting a control program configured to run on the PLC. (Specification at page 1, lines 14-16). PLCs may be accessed on the factory floor through special controls or by connecting a laptop to the PLCs. (Specification at page 1, lines 17-22). PLCs may also be connected to an Ethernet network or other type of network to enable the control program of the PLC to be adjusted remotely. (Specification at page 1, lines 23-29).

Where the PLCs are able to be accessed over a network, a network user intending to modify the program of one particular PLC may inadvertently modify the program of a different PLC. (Specification at page 1, line 30 to page 2, line 1). Likewise, having the PLCs connected to the network makes the PLCs susceptible to network malfunctions and attacks, and enables maleficent individuals to change the manner in which the factories are operating on the factory floor. Mistakenly changing the way a machine operates by accessing the wrong PLC, or intentionally changing the way a machine to operate improperly may cost the factory money and may be physically dangerous to people working on the factory floor. (Specification at page 2, lines 1-10).

Accordingly, applicants proposed to enable security policy to be implemented on the PLCs to enable the PLCs to take advantage of network authentication, authorization, and other network services, while enabling local policy enforcement and allowing local policy overrides where necessary. (Specification at page 2, lines 13-16). This enables security policy to be implemented at the PLC, e.g. via a Security Policy Implementation Point (SPIP), which implements controlled access of the PLC and attendant factory machines from the network. (Specification at page 2, lines 16-19).

The following tables map support in the specification to the claim limitations:

Independent Claim 1:

Claim limitation	**Support**
1. An industrial network, comprising	Fig. 1, element 10; Specification at page 4, lines 28-29
a local area network	lines interconnecting boxes in Fig. 1; specification at page 4, lines 22-24; specification at page 7, lines 23-25

one or more programmable logic controllers; and	Fig. 1, element 14; specification at page 5, lines 3-6; Fig. 2; specification at page 5, line 26 to page 6, line 19
a security policy implementation point (SPIP) connected between the local area network and the one or more programmable logic controllers to isolate the one or more programmable logic controllers and associated factory machines from the local area network	Fig. 1, element 22; specification at page 6, lines 20-22, page 7, lines 1-11; Fig. 3; specification at page 7, line 26 to page 8, line 4
to prevent a person using a management program from accessing the one or more programmable logic controllers over the local area network unless authenticated to the SPIP and authorized to take action on the one or more programmable logic controllers isolated by the SPIP,	Fig. 3, authentication module 56; specification at page 9, lines 15-24
the SPIP being configured to participate in a Virtual Private Network (VPN) such that communications between the management program and the SPIP over the industrial network occur over a VPN tunnel.	Fig. 3, VPN module 64; Specification at page 9, line 27 to page 10, line 6

Independent Claim 14:

Claim limitation	**Support**
14. A Security Policy Implementation Point (SPIP) for use in an industrial network, comprising:	Fig. 1, element 22; specification at page 6, lines 20-22, page 7, lines 1-11; Fig. 3; Fig. 3; specification at page 7, line 26 to page 8, line 4

a local path to implement a local access policy related to direct local access to one or more programmable logic controllers; and	Fig. 3, local input 66; specification at page 10, line 17 to page 11, line 14
a network path connected between the industrial network and the one or more programmable logic controllers to control access to the programmable logic controller via the industrial network, the network path isolating the one or more programmable logic controllers and associated factory machines from the industrial network to prevent a person using a management program from accessing the one or more programmable logic controllers over the local area network unless authenticated to the SPIP and authorized to take action on the one or more programmable logic controllers protected by the SPIP, the network path also implementing a Virtual Private Network such that communications with the SPIP over the industrial network occur over a VPN tunnel.	Fig. 3, network ports 44; specification at page 8, lines 8-13; Fig. 5, element 88, specification at page 12, lines 13-28 Fig. 3, authentication module 56; specification at page 9, lines 15-24; Fig. 5, element 90; Specification at page 12, line 29 to page 13, line 10 Fig. 3, VPN module 64; Specification at page 9, line 27 to page 10, line 6

(vi) Grounds of Rejection to be Reviewed on Appeal.

Whether claims 1-3, 7, 9-11, 13-15, 17-18, and 21-22 are unpatentable under 35 USC 103 over Hamilton (U.S. Patent No. 7,123,974) in view of Daniely (U.S. Patent No. 6,763,469).

Whether claims 4-6 and 23-25 are unpatentable under 35 USC 103 over Hamilton in view of Daniely, and further in view of Danner (U.S. Patent No. 7,194,003).

Whether claim 16 is unpatentable under 35 USC 103 over Hamilton in view of Daniely, and further in view of Schmitz (U.S. Patent No. 6,172,430).

Whether claims 19-20 are unpatentable under 35 USC 103 over Hamilton in view of Daniely, and further in view of Amara (U.S. Patent Application Publication No. 2004/0083295).

(vii) Argument

Independent claim 1, and dependent claims 2-3, 7, 9-11 and 13

As noted above, this application relates to industrial networks, and more particularly to a way in which access to particular PLCs and attendant factory machines may be circumscribed so that only particular authorized individuals may have access to particular PLCs over the industrial network.

As discussed in the background of the specification, for example at page 1, PLCs are able to be connected to a company's Ethernet network or other data network. However, where there is more than one person that is allowed to program PLCs on the network, a person may accidentally make a change to the wrong PLC or a person may intentionally change the programs of PLCs on the network to cause the machines associated with the PLCs to operate incorrectly.

Accordingly, applicants proposed to implement a security point (Secure Policy Implementation Point – SPIP) between the network and the PLC to control who is allowed to access particular PLCs via the network. Thus, simply obtaining access to a centralized network controller or central management program is insufficient to program all PLCs connected to the network – the SPIP will also require that the user of the network control system be authenticated and authorized at a particular SPIP before allowing the user to make changes to the PLCs associated with the SPIP.

Hamilton teaches a system in which an "access tool 510" is able to keep a record of what actions are taken on PLCs over the network. Hamilton does not teach a system that can prevent access to a particular PLC, but rather simply teaches that access should be recorded. (see e.g. Hamilton at Fig. 10).

In the Office Action, the Examiner cited Hamilton as teaching a local area network interconnecting programmable logic controllers on the network. (See Office Action at page 2). The Examiner contends that Hamilton teaches a Security Policy Implementation Point (SPIP) between the network and the programmable logic controllers. Id. As support for this position,

the Examiner has cited Hamilton at Figs. 1, 2, and 6, and more particularly Fig. 6, col. 9, lines 7-33.

In Fig. 6, and the associated text at Col. 9, lines 7-33, Hamilton shows a system 500 illustrating security operations. In the second sentence of the paragraph (Col. 9, lines 8-9), Hamilton states that an "access tool 510" has one or more security layers 520. In Hamilton, the term "access tool" is used to refer to the management program that is used to interact with the PLCs on the network (see Col. 4, lines 60-61). Thus, Fig. 6 and the text at col. 9, lines 7-33 is unrelated to a SPIP, but rather teaches that the management tool, which is used to interact with the PLCs, should have one or more security layers. Accordingly, contrary to the Examiner's assertion, this portion of Hamilton does not teach or suggest a SPIP associated with the PLC, but describes a management program. Thus, the "access tool 510" may be considered to correspond with the central control described by applicants and which would be used by a programmer to access particular PLCs on the network. (see specification at page 1, line 30 to page 2, line 1 and page 9, lines 25-26). As noted above, applicants were looking to restrict access by a programmer so that, even though the programmer was authorized to use the central control, the programmer would need to have particular authorization/authentication at a SPIP associated with a PLC to have access to the PLC. Thus, the SPIP represents a separate layer of control apart from whatever security may be provided by the management tool.

On page 3 of the Office Action the Examiner further cited col. 10, lines 45-60 of Hamilton as providing support for the position that Hamilton teaches a SPIP connected between the network and the PLCs. At Col. 10, lines 45-60, Hamilton teaches that applications can communicate with the PLCs, and control the PLCs. This relates to how PLCs can be controlled on the network, but does not mention or suggest the use of a separate layer of control in the form of a SPIP interposed between the PLC and the network to prevent a person having access to the management program from accessing particular PLCs on the network.

In the "Response to Amendment" section, the Examiner indicated that Hamilton teaches a management program that accesses one or more controllers over the network (Office Action at Page 13, lines 7-10). Applicants agree that Hamilton teaches a management program. This statement by the Examiner actually supports applicants' position which is that Hamilton teaches a management program rather than both a management program and SPIPs that prevent a person from using the management program to access particular PLCs.

The Examiner focuses on the monitoring aspect of Hamilton as corresponding to the claimed SPIPs. This was legal error, since the monitoring aspect of Hamilton does not perform the functions attributed to the SPIP in this application.

In Hamilton, whenever a person interacts with a PLC, the access is recorded as "activity data." (see Col. 5, lines 4-23). Hamilton is focused on recording what takes place with the PLCs, and the data that is collected in connection with this is referred to as activity data. In the "Response to Arguments" section the Examiner stated, that Hamilton teaches an Access Tool to "monitor the interaction over the network." (Office Action at page 13, lines 10-11). Applicants describe a similar feature in connection with logging activity on the network. Specifically, applicants describe in connection with Fig. 6 that a central logging facility 104 should be used to keep track of the various control actions taken by people whenever a person accesses a PLC. (See Specification at page 10, lines 7-16, and page 12, line 23 to page 13, line 18). Thus, applicants, like Hamilton, teach a system that can log actions taken by users in connection with programming the PLCs.

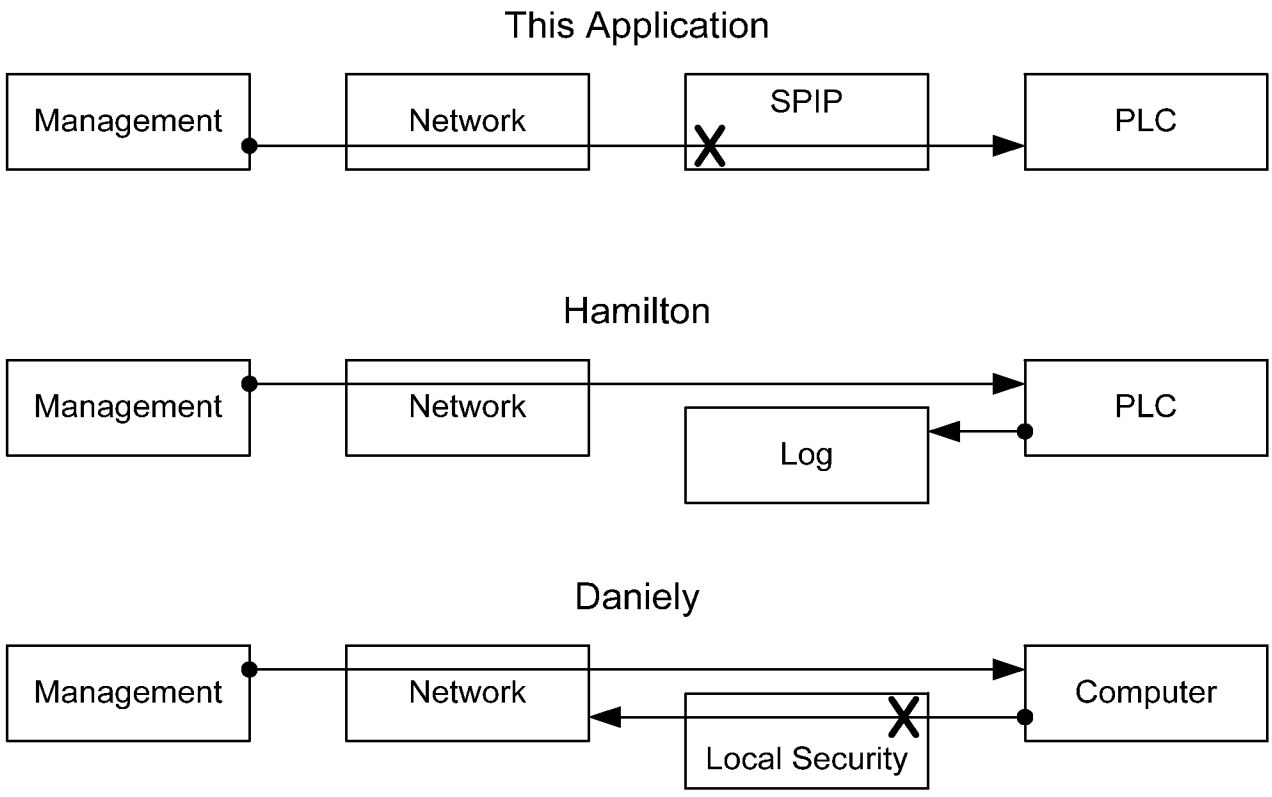
In Hamilton, once a change is made to the PLC, the change is logged and information associated with the change is forwarded over the network. Hamilton secures this data on the network as noted by the Examiner. (O.A. at page 13, lines 11-16). However, the fact that the record of the interaction between the user of the management system and the PLC is secured does not mean that the user of the management system was prevented in the first instance from having access to the PLC. Rather, the opposite is true – once the access data exists the person has necessarily had access via the management system to the PLC.

The flaw in the Examiner's logic is manifest in the Office Action at page 13, lines 16-20. Specifically, the Examiner states that the fact that access data is recorded means that the "access tool" is a security policy implementation point (SPIP) that protects the one or more PLCs from unauthorized access. There are two problems with this. First, as noted above, the "access tool" corresponds to the management program. Thus, the "access tool" is not a SPIP. Specifically, claim 1 recites that the SPIP "prevent a person using a management program from accessing the one or more programmable logic controllers over the local area network unless authenticated to the SPIP." Since the SPIP presents a person using a management program from having access to the PLC, the SPIP necessarily must be different than the management program.

Second, the access tool in Hamilton records access to the PLCs, it does not protect the PLCs against unauthorized access. Thus, the "access tool" in Hamilton also does not perform the recited function of preventing a person using a management program from accessing the one or more PLCs. Accordingly, applicants respectfully submit that the Examiner committed reversible error by misinterpreting the teachings of Hamilton. Specifically, Hamilton does not teach or suggest a system in which SPIPs provide access control to prevent a management program from accessing the particular PLCs.

The Examiner cited Daniely as teaching a SPIP connected between the local area network and one or more computers. Thus, the Examiner contends that Daniely makes up any deficiencies of Hamilton. Daniely shows a security system in which a local security device is used to protect each computer connected to the network. For example, in Fig. 1A of Daniely, a local security device 20 is connected between each computer 22 and the network. The local security device is used to control what a user (using the computer) can do on the network. (Daniely at Col. 4, lines 1-12). Daniely defines the term "computer" to include personal computers or other devices that have an operating system such as a DOS, Windows, Linux, or other operating system (Daniely at Col. 3, lines 9-29). Thus, Daniely is not related to protecting PLCs on the networks, but rather shows that each computer on a computer network (such as the computer running a PLC management program) may have a local security device to control its actions on the network and to control which other computers on the network have access to it. (See e.g. Daniely at Col. 6, lines 24-52).

This is opposite what is being done in this case. Applicants have created the following illustration to show operation of this application in comparison with Hamilton and Daniely



As may be seen in this figure, applicants have a SPIP interposed between the network and the PLC to prevent a management program from accessing the PLC. Hamilton does not have a system of this nature, but rather has a log program on the network that keeps track of whenever the management system accesses the PLC. Daniely likewise does not prevent the management system from accessing the computer, but rather has a local security component that prevents the computer from taking action on the network. Thus, neither reference teaches or suggests using a device to prevent a management system from having access to a PLC or other computer component.

Claim 1 recites "a security policy implementation point (SPIP) connected between the local area network and the one or more programmable logic controllers to isolate the one or more programmable logic controllers and associated factory machines from the local area network to prevent a person using a management program from accessing the one or more programmable logic controllers over the local area network unless authenticated to the SPIP and authorized to take action on the one or more programmable logic controllers isolated by the SPIP. Since neither cited reference teaches or suggests this concept, the Examiner committed legal error by rejecting independent claim 14 under 35 USC 103 over the combination of Hamilton and

Daniely. Accordingly, the Examiner's rejection of independent claim 1 and those claims dependent thereon should be reversed.

Independent claims 14 and dependent claims 15-25

The discussion of Hamilton and Daniely is incorporated in this section by reference. Claim 14 recites a SPIP that includes "a network path connected between the industrial network and the one or more programmable logic controllers to control access to the programmable logic controller via the industrial network. The combination of Hamilton and Daniely does not disclose this concept. Further, claim 14 recites that the network path isolates "the one or more programmable logic controllers and associated factory machines from the industrial network to prevent a person using a management program from accessing the one or more programmable logic controllers over the local area network unless authenticated to the SPIP and authorized to take action on the one or more programmable logic controllers protected by the SPIP."

Since neither cited reference teaches or suggests this concept, the Examiner committed legal error by rejecting independent claim 1 under 35 USC 103 over the combination of Hamilton and Daniely. Accordingly, the Examiner's rejection of independent claim 14 and those claims dependent thereon should be reversed.

(viii) Claims Appendix

An appendix containing the current version of all pending claims is attached.

(ix) Evidence Appendix

None.

(x) Related Proceedings Appendix

None.

Conclusion

Applicants respectfully request that the rejection under 35 U.S.C. 103 over Hamilton in view of Daniely be reversed. The other rejections which rely on the combination of Hamilton and Daniely in view of one or more secondary references should likewise be reversed because of

the deficiency in the combination of Hamilton and Daniely.

Applicants request any required extension of time to enable this brief to be considered timely. Payment of the fee for filing this Appeal Brief and any required extension of time fees is being submitted herewith. If any additional fees are due in connection with this filing, the Commissioner is hereby authorized to charge payment of the fees associated with this communication or credit any overpayment to Deposit Account No. 141315 (Ref: 15929ROUS02U).

Respectfully Submitted

Dated: June 8, 2009

/John C. Gorecki/
John C. Gorecki, Reg. No. 38,471

Anderson Gorecki & Manaras LLP
P.O. Box 553
Carlisle, MA 01741
Tel: (978) 264-4001
Fax: (978) 264-9119

APPENDIX – PENDING CLAIMS

1. An industrial network, comprising:

a local area network;

one or more programmable logic controllers; and

a security policy implementation point (SPIP) connected between the local area network and the one or more programmable logic controllers to isolate the one or more programmable logic controllers and associated factory machines from the local area network to prevent a person using a management program from accessing the one or more programmable logic controllers over the local area network unless authenticated to the SPIP and authorized to take action on the one or more programmable logic controllers isolated by the SPIP, the SPIP being configured to participate in a Virtual Private Network (VPN) such that communications between the management program and the SPIP over the industrial network occur over a VPN tunnel.

2. The industrial network of claim 1, wherein the SPIP is integrated with the programmable logic controller and wherein the SPIP is logically connected between the local area network and the one or more programmable logic controllers.

3. The industrial network of claim 1, wherein the network contains a plurality of programmable logic controllers, wherein the one or more programmable logic controllers are a subset of the plurality of programmable logic controllers, and wherein the SPIP is physically disposed between the local area network and the one or more programmable logic controllers.

4. The industrial network of claim 3, wherein the local area network is an Ethernet network, wherein the SPIP is configured to communicate with network devices on the local area network over the Ethernet network, and wherein the SPIP is configured to communicate with the programmable logic controller using a protocol selected from at least one of Profibus, Controller Area Network, RS-232, RS-422, and RS-485.

5. The industrial network of claim 1, wherein the local area network includes at least one Ethernet switch/router, and wherein the SPIP is included as a blade in the Ethernet switch/router.

6. The industrial network of claim 5, wherein the SPIP is configured to implement security policy to control network access to at least one PLC connected to the Ethernet switch/router through the SPIP.

7. The industrial network of claim 1, wherein the SPIP is further configured to apply policy to limit access to the programmable logic controllers to individuals authorized to access the programmable logic controllers and to require authentication on the SPIP before allowing control instructions to pass from the local area network through the SPIP to the one or more programmable logic controller.

8. (Canceled)

9. The industrial network of claim 1, wherein the industrial network is an untrusted network configured to interconnect network services with a plurality of SPIPs associated with factory machines, and wherein the network services are configured to enable operation of the factory machines to be altered through the industrial network.

10. The industrial network of claim 1, wherein the SPIP is further configured to enable local access to the one or more programmable logic controllers by applying local authentication and authorization policy to enable the SPIP to enforce network policy in connection with attempted local access.

11. The industrial network of claim 10, wherein the local policy comprises:

a local access policy configured to require authentication and authorization of at least one of an user and an accessing electronic device for non-emergency attempts to access the SPIP, and

an alternate access policy configured to allow access to the SPIP and maintain an audit log attendant to a local attempt to access the SPIP.

12. (Canceled)

13. The industrial network of claim 1, wherein the SPIP comprises a local authentication policy and information associated with authorized users and indicative of authorization policy information associated with said at least one factory machine.

14. A Security Policy Implementation Point (SPIP) for use in an industrial network, comprising:

a local path to implement a local access policy related to direct local access to one or more programmable logic controllers; and

a network path connected between the industrial network and the one or more programmable logic controllers to control access to the programmable logic controller via the industrial network, the network path isolating the one or more programmable logic controllers and associated factory machines from the industrial network to prevent a person using a management program from accessing the one or more programmable logic controllers over the local area network unless authenticated to the SPIP and authorized to take action on the one or more programmable logic controllers protected by the SPIP, the network path also implementing a Virtual Private Network such that communications with the SPIP over the industrial network occur over a VPN tunnel.

15. The SPIP of claim 14, further comprising programmable logic controller circuitry configured to implement the one or more programmable logic controllers and to function to control at least one factory machine.

16. The SPIP of claim 15, wherein the local access policy includes enabling access to an associated factory machine to enable operation of the factory machine to be altered without verification of authorization and authentication of an user seeking to alter the operation during an emergency.

17. The SPIP of claim 16, wherein the local path further comprises an accounting module configured to record accesses to at least one of the SPIP, an associated programmable logic controller, and an associated factory machine.

18. The SPIP of claim 15, wherein the local path comprises an authentication module configured to authenticate the identity of an individual seeking to access a device through the SPIP, and an authorization module configured to assess an authorization associated with the individual to ascertain whether the individual is authorized to access the device.

19. The SPIP of claim 18, wherein the authorization module is an interface to a Lightweight Directory Access Protocol (LDAP) server, and wherein the authentication module is an interface to a Remote Access Dial In User Service (RADIUS) server.

20. The SPIP of claim 18, wherein the authentication and authorization modules maintain a local copy of authorized users and authentication policy to allow local access to the SPIP.

21. The SPIP of claim 15, wherein the SPIP is configured to apply policy to limit access to the programmable logic controllers to individuals authorized to access the programmable logic controllers and to require authentication on the SPIP before allowing control instructions to pass from the industrial network through the SPIP to the one or more programmable logic controllers.

22. The SPIP of claim 15, further comprising network ports configured to interface with the industrial network, and output ports configured to interface with a programmable logic controller.

23. The SPIP of claim 22, wherein the network ports are configured to communicate on the industrial network utilizing an Ethernet protocol; and wherein the output ports are configured to communicate with the programmable logic controller using a protocol understandable by the programmable logic controller.

24. The SPIP of claim 15, further comprising network ports configured to interface with the industrial network, control logic configured to implement a control program associated with a programmable logic controller, and interface ports configured to interface with a factory machine.

25. The SPIP of claim 24, wherein the interface ports comprise at least one input port configured to receive input from an environmental sensor, and at least one output port configured to control at least one electro-mechanical device.